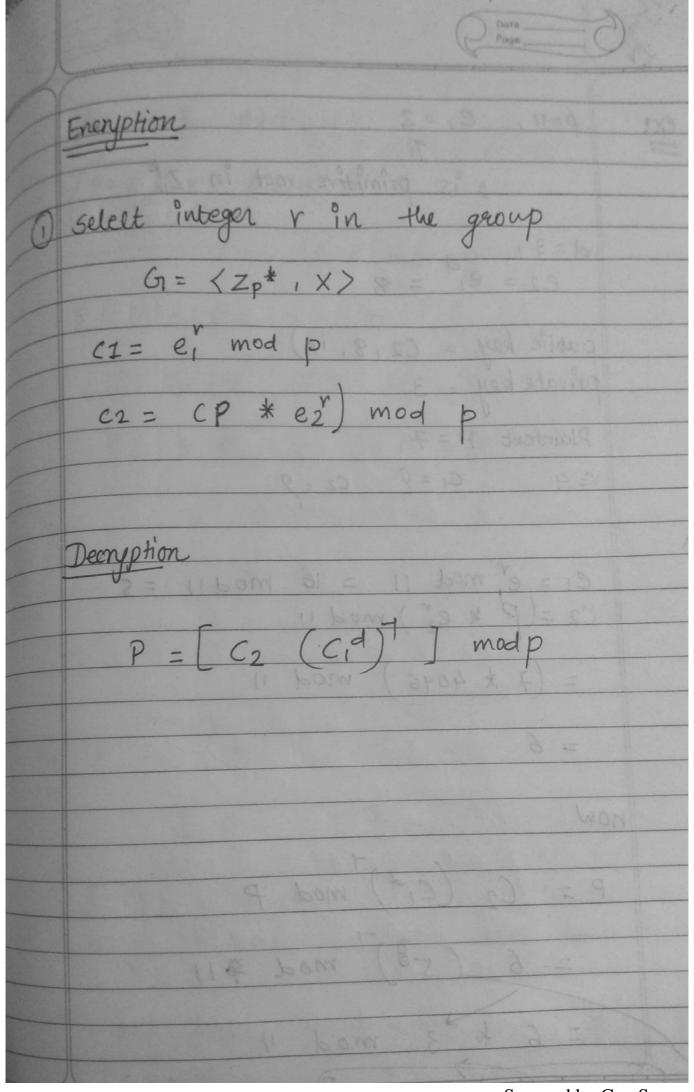
	order of element $a' = x \pmod{n}$ $G = \langle \mathcal{G}_{+}^{*}, x \rangle$
121,213	i = order of element
	Primitive Root
	Group Gi = < Zp* , x>
	order of Group pcp)
	REAL RESIDENCE
Where	$\phi(i) = 0$ $\phi(p) = p + i $ p is prime
	d(m xn) = d(m) + d(n)
	m & n are relatively prime
	& cpe) = pe - pet
	it pis point
	THE RESIDENCE OF THE PARTY OF T
=)	In the group, $G_1 = \langle Z_n^*, \chi \rangle$
	when the order of element is the same as $\phi(n)$,
	that element is called the
3	primitive root of the grap.

Scanned by CamScanner

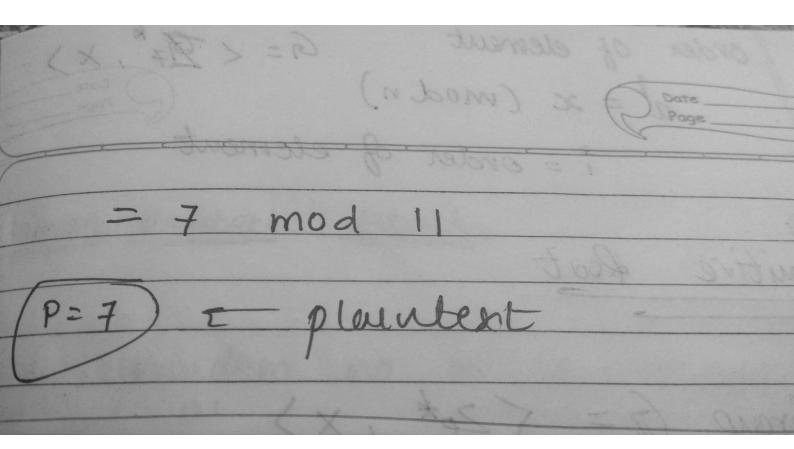
2,* -> set of all relative primes of X = Y (modn) * Elgamal Cryptosystem Key Generation O select a large prime p 2) select d to be a member of the group $G = \langle Z_p^*, \chi \rangle$ Such that 1 \d \ p-2 select e, to be primitive voot in

the group $G = \langle z_p^*, \chi \rangle \longrightarrow \phi(p)$ $a^i = \chi(mod n)$ ez = eid mod p public key = Ze1, e2, p3 L9, x, 44) private key = d.



P=11, 61=2 g is primitive voot in Zit e2 = e, = 8 public key = (2,8,11) private key = 3 Plaintext P = 7 V= 4 C1=9 C2=9 C1 = e, mad 11 = 16 mod 11 = 5 C2 = (p * e2) mod 1) = (7 * 4096) mod 11 now P = C2 (C14) mod P = 6 (58) mod \$11 = 6 to 3 mod 11 (125 * (3) mod 11 = 1) L multiplicative module

Scanned by CamScanner



* known-plaintext Attack Same vandom no se to encrypt two plaintext P' can be discovered by using P' C2 = P x(e2) mod p c2' = p' x e2 mod p (2°) = C2 X pt mod p c' x cezy) mod p